

** For Examiner's Reference **

CLAIMS WITH INTERSTITIAL REFERENCES

FOR DISCUSSION PURPOSES ONLY

CLAIMS

What is claimed is:

(Claims 1-8 are Figs. 13a and 13b:)

1. A method of providing a secure data stream between system nodes U_s and U_d , the method comprising:

encrypting data at a node U_s with an encryption key DSK'_i ;
selecting encrypted data (176, 172) and
regenerating a new encryption key (180) at a node U_s with an encryption key (170) and selected encrypted data (172)

2. The method of claim 1 wherein the step of selecting encrypted data comprises selecting encrypted data (176, 172) using a byte from a previous encryption key (170) as a seed of random generation (176).

3. The method of claim 1 wherein the step of regenerating a new encryption key comprises regenerating a new encryption key (180) by performing a logic operation on a previous encryption key (170) and selected encrypted data (172).

4. The method of claim 3 wherein the step of regenerating a new encryption key by performing a logic operation comprises regenerating a new encryption key (180) by performing an XOR logic operation on a previous encryption key (170) and selected encrypted data (172).

5. The method of claim 3 wherein the step of regenerating a new encryption key by performing a logic operation comprises performing a logic operation on a previous encryption key **170** and selected encrypted data **172** to form an expanded key **174**

6. The method of claim 5 further comprising the step of selecting bytes **178** from an expanded key **174** to generate the new encryption key **180**.

7. The method of claim 6 wherein the step of selecting bytes **178** from an expanded key **174** to generate the new encryption key **180** comprises randomly selecting bytes **178** from an expanded key **174** to generate the new encryption key **180**.

8. The method of claim 7 wherein the step of randomly selecting bytes **178** from an expanded key **174** to generate the new encryption key **180** comprises randomly selecting bytes from an expanded key **174** using a byte from a previous encryption key **170** as a seed of random generation **176**.

(Claims 9 – 13 are Fig. 11:)

9. The method of claim 1 further comprising the step of encrypting data **146** with a new encryption key **148**.

10. The method of claim 9 wherein the step of encrypting data **146** with a new encryption key **148** comprises performing a logic operation on the data **146** and new encryption key **148**

11. The method of claim 10 wherein the step of performing a logic operation on the data **146** and new encryption key **148** comprises performing an XOR operation on the data **146** and new encryption key **148**.

12. The method of claim 10 wherein the step of performing a logic operation on the data **146** and new encryption key **148** comprises forming a cipher **150**.

13. The method of claim 12 further comprising the step of permuting portions of the cipher **152**, **154** to form another cipher **156**.

(Claim 14 is Fig. 8:)

14. The method of claim 9 further comprising the step of transmitting **104** encrypted data over a data stream.

(Claims 15 – 16 are Fig. 9:)

15. The method of claim 14 further comprising the step of receiving encrypted data **118** at a destination node U_d .

16. The method of claim 15 further comprising the step of decrypting encrypted data **120** at the destination node U_d .

(Claim 17 is Fig. 12:)

17. The method of claim 16 wherein the step of decrypting encrypted data comprises decrypting with a decryption key **166**.

(Claim 18 is Figs. 13a and 13b:)

18. The method of claim 17 further comprising the step of regenerating a new decryption key **(Fig. 13)** using selected decrypted data **168** and a previous decryption key **166**.

19. A system for providing a secure data stream between a source programmable apparatus and a destination programmable apparatus, the system comprising:

- a source programmable apparatus U_s ;
- a data stream created by said source programmable apparatus;
- means for encrypting data **172** of said data stream with an encryption key **DSK 170**; and
- means for regenerating a new encryption key **180** using selected previously encrypted data **172**.

20. The system of claim 19 further comprising:

- a destination programmable apparatus U_d in electrical communication with said source programmable apparatus U_s ;
- means for transmitting encrypted data **158** to said destination programmable apparatus;
- means for decrypting said encrypted data **158** received at said destination programmable apparatus U_d with a decryption key **166**; and
- means for regenerating a new decryption key **180** using selected previously decrypted data **172**.